REVISTA SAN GREGORIO

Criminal Prosecution of Persons, Who Committed Criminal, Acts Using the Cryptocurrency in the Russian Federation

Enjuiciamiento penal de personas que cometieron actos delictivos utilizando la criptomoneda en la Federación de Rusia

Authors
Viktor Victorovich Pushkarev[1], Valeriia Valerievna Artemova[2], Sergey Vyacheslavovich Ermakov[3], Elmir Nizamievich Alimamedov[4], Anton Valerevich Popenkov[5]

[1]Plekhanov Russian University of Economics, Moscow, RUSSIA
[2]Moscow University of the Ministry of Internal Affairs of Russia named by V.Ya. Kikot, Moscow, RUSSIA
[3]Moscow University of the Ministry of Internal Affairs of Russia named by V.Ya. Kikot, Moscow, RUSSIA
[4]Finance University under the Government of the Russian Federation, Department of Legal Regulation of Economic Activities, Moscow, RUSSIA
[5]Moscow University of the Ministry of Internal Affairs of Russia named by V.Ya. Kikot, Moscow, RUSSIA

Fecha de recibido: 2020-11-07
Fecha de aceptado para publicación: 2020-12-10
Fecha de publicación: 2020-12-15

Abstract
The law enforcement agencies' main focus aimed at combatting crimes, which were committed with the use of cryptocurrency include struggling and prevention of illegal entrepreneurship, illegal banking activity, tax crime, illegal capital outflows, drug business, terrorism financing, legalization (laundering) of income. These crimes are significantly urgent not only in the Russian Federation, but in the whole world, as they provide further criminal economy's and corresponding institutions' development (i.e. corruption, illegal immigration, etc.). Thus, the topicality and practical importance of elaborating the methods aimed at crime investigation are doubtless.

Keywords: criminal prosecution, pre-trial proceedings, prosecutor, cryptocurrency, digital rights, digital economy.

Resumen
El principal enfoque de las agencias de aplicación de la ley dirigido a combatir los delitos, que se cometieron con el uso de criptomonedas, incluye la lucha y la prevención del emprendimiento ilegal, la actividad bancaria ilegal, los delitos fiscales, la salida ilegal de capitales, el negocio de las drogas, el financiamiento del terrorismo, la legalización (lavado) de ingresos. Estos delitos son muy urgentes no solo en la Federación de Rusia, sino en todo el mundo, ya que contribuyen al desarrollo de la economía criminal y de las instituciones correspondientes (es decir, corrupción, inmigración ilegal, etc.). Así, es indudable la actualidad e importancia práctica de la elaboración de los métodos destinados a la investigación del delito.
Palabras clave: proceso penal, diligencia previa, fiscal, criptomoneda, derechos digitales, economía digital.

Introduction

The inclusion of digital rights and assets leads to high risks, which threaten economic systems' normal functioning, undermine the economic security and can facilitate organized crime, such as corruption and terrorism financing.

According to the US mass-media official reports, in 2017 around 266 million dollars have been laundered in the field of digital economic relations in the USA. In 2018 around 1,5 billion dollars were laundered (Crypto money laundering up threefold in 2018).

The digital economy crimes are highly latent, organized and exterritorial and the ways of committing them are being constantly improved.

Under such conditions the economy, being transformed, promotes public relations' criminal features, which reflect the economic crimes global vector which is cybercrime. This new type of crime is not only closely connected with the information security issues in the public and private interests' spheres, but with the problems, threatening the whole financial system as well.

As the traditional economy, the digital economy cannot exist without a universal value equivalent, which is supposed to denote digital assets and rights, widely spread as the cryptocurrency, tokens and stablecoins, which in turn will be viewed from their marginal features' point of view.

Materials and Methods

The cryptocurrency is either the subject or the means of crime, although, the practice of investigating the cryptocurrency crimes is insignificant. This fact is due to the complicated economic crimes' novelty, insufficient legal regulation, operations' anonymity and the problems of detecting them in the information-telecommunication space. However, the increasing interest causes the cryptocurrency's spreading and consequently ways of committing crimes with it.

The study's empirical base includes the results of: 58 criminal cases heard in various Russian Federation regions; surveys of 35 prosecutors, working in the Ministry of Internal Affairs Investigation Department and the Ministry of Internal Affairs Central Investigations Office in Moscow city; surveys of 23 persons of the teaching personnel at the Ministry of Internal Affairs Administration Academy, the Moscow Ministry of Internal Affairs University, named after V. Kikot and the Saint-Petersburg Ministry of Internal Affairs University.

The analytical legal research method has been chosen to work with the research data, as it allows generalizing the results of applying special juridical methods. The comparative law method has allowed studying and defining the Russian Federation's Criminal Code and the international regulatory legal acts' common provisions. When studying criminal cases and interviewing the law enforcement officials the sociological method has allowed discovering, analyzing, systematizing and summarizing the results of empirical investigations. The formal-juridical has helped characterizing the whole situation around the investigation of cryptocurrency crimes in Russia. This has helped developing the typology of ways of committing such crimes, forming the scientific idea of cryptocurrency crimes, analyzing and classifying the pre-trial and criminal proceedings' problems and suggesting the ways to solve them.

Results Analysis

1. Crimes, connected with the cryptocurrency mining are distributed into electricity theft and mining equipment theft.

A. A criminal case is initiated, basing on the resources owner' (resources supplier) claim or the energy company, which legally redistributes the energy between the consumers. The company's authorized representatives' submit a claim, stating that the energy loss has been detected and that it has caused large-scale damage, which is more than 250 thousand rubles, according to Article 165 Pt.2 of the Russian Federation's Criminal Code.

The crime scene inspection allows discovering the plugged in mining equipment and power supply cables, connected to the power substation without metering devices. The amount of damage caused is measured by a specialist, who applies electricity tariffs, approved by competent authorities for the period when the electricity has been stolen, and a standard consumption indicator, which is used if there no metering devices installed.

B. A criminal case is initiated, basin on the stolen equipment owner's claim.

An investigator examines the version of stealing the electricity, than asks the energy company to submit the information on electricity consumption at the crime scene.

If the equipment, which has never been used for mining the cryptocurrency, is stolen, then the investigator is entitled to ask the energy company to submit the information on a rapid energy

consumption increase in order to discover whether the stole equipment has ever been used (an ASIC consumes from 2,5 to 5 kWh).

2. Crimes, where the cryptocurrency or fiat currency is involved. The cryptocurrency's physical exchange is the main drawback in the cryptocurrency's circulation ecosystem and provokes such crimes as fraud, extortion, theft or robbery. Victims' statements (usually individuals' statements) serve as the reasons for initiating criminal cases.

A. Unidentified persons misled the victim and assured him that they can help selling 103 bitcoins. The victim gave the unidentified persons the cryptocurrency at the cost of 45.3 million rubles in an office, wherefrom they further escaped.
B. The robbers attacked the victim, stole his cryptocurrency, transferred it to the bank account, cashed it and used it at their own discretion. After a thorough inspection the case was forwarded to court.

C. Three unidentified persons beat the victim, out him in a car and demanded transferring 300 bitcoins to another account. When the victim did everything that was demanded, the unidentified persons stole his bag, where there were the victims belongings, documents, a laptop, two cell phones and 20 thousand US dollars.
In such cryptocurrency cases the investigator has to pay special attention to getting the information on the e-wallets, involved in the money transfer, was of transferring it and detecting the traces of such operations on the technical equipment used. The information is further fixed in the declarer's protocol statement. The technical equipment is in turn checked by an expert.

D. A. Smirnova, acting according to her criminal role, known under pseudonym "Alena", wrote to D. Yerofeev on "Telegram" and said that she wanted to buy a big amount of cryptocurrency. D. Yerofeev agreed to meet Alena and sell her the cryptocurrency. When they met D. Motorin snatched D. Yerofeev's IPhone 7 with the "Blockchain" programme in order to steal his bitcoins. D. Motorin demanded from D. Yerofeev to transfer the bitcoins to his special e-wallet. D. Yerofeev unblocked his phone and entered his "Blockchain" account. After that using D. Yerofeev's "Blockchain" account D. Motorin transferred 2.8 bitcoins to the e-wallet owned by the criminal group.

The following evidence has been collected at the initial investigation stage:

- A disc with CC-TV recordings;
- "Telegram" correspondence;
- Website correspondence;
- The exchange account screenshot;
- The "Blockchain" website screenshot;
- The bitcoins transfer screenshot;
- The screenshots of the "Blockchain" private accounts of the victim and suspect
- A screenshot of the bitcoins received by the suspect;
- The suspect's Sberbank bank account statement.

The abovementioned evidence was enough to charge the suspects with the crime, end the pre-trial proceedings, draw up the indictment and convict the criminals.

3. The cryptocurrency theft. A criminal case is initiated after the victim submits the claim. An investigator has to get full information from the victim on the cryptocurrency's origin, circumstances of the transfer and the whole criminal case. Screenshots are preferable.

An unidentified person living in 7, Aivazovskogo St, Flat 4, Leninskii District, Sevastopol, has secretly stolen 8 bitcoins, which equal 35 thousand rubles damage to V. Kalyunas.
B. An unidentified person illegally entered the atoris-h@mail.ru email box, registered in the name of B. Sharifov and his account at the bittrex.com website, wherefrom this unidentified person stole the amount of cryptocurrency equal to 400 thousand rubles.

An expert, who could detect the transaction, was not questioned, so it was impossible to find out the transaction time and receiver. All these and certain other facts have led to the preliminary investigation suspension, based on Article 208, Part 1, Clause 1 of the Russian Federation Criminal Procedure Code.
4. Fraud under the pretext and\ or with use of cryptocurrency.

On the 12th, March 2017 in between 12 and 6 p.m. Ye. Ovchinnikova, working in an office №15 on the 93, Leningradskaya St., Biisk, The Altai Krai, held a meeting with Biisk citizens and the "OneCoin" company partners. At the meeting Ye. Ovchinnikova misled the audience and deliberately gave false information on registering a shared pool (private account) on the www.onelife.eu website, which belongs to the "OneCoin" company. Further, she planned to purchase the cryptocurrency at a profitable price of 31 hundred thousand rubles. Ye. Ovchinnikova said to the audience that they had to donate 31 thousand rubles (one hundredth of the whole pool) and either give the money to her or transfer it to her son's bank account.

Ye. Ovchinnikova's surrender and confession served as the reason for initiating the criminal case. The inspection of all bank accounts, bank cheques (cheques of all transfers) and the www.onelife.eu correspondence screenshots were enough to draw up the indictment.
B. An unidentified person called G. Ivanov, living in Kstovo, Nizhnii Novgorod Oblast, and suggested taking part in the cryptocurrency trade. The stolen money, which G. Ivanov gave, were further transferred to an account at "BitXchange".

4. The use of the cryptocurrency as a means of committing a crime.
A. A criminal case under Article172, Part 2 of the Russian Federation Procedure Code was initiated in Kostroma Oblast. The detainees cashed 500 million rubles by exchanging and transferring the cryptocurrency. They registered more than 300 bank and SIM-cards to exchange and transfer the cryptocurrency.

B. An unidentified person, who organized the criminal group, spread the malware and thus stole users' private banking information. He submitted this information to the internet resource, which were available to his fellow-criminals and M. Dzhumayev in particular. Later M. Dzhumayev and unidentified persons used the stolen private information and electronic devices to transfer the money to other people involved in the crime, who in turn cashed the stolen money for their future use. After that they exchanged the money for bitcoins on special shadowy Internet resources and transferred it to the bitcoin e-wallets belonging to M. Dzhumayev.

5. Fraud with the use of cryptocurrency in the information and telecommunications space.
A. Fraud when investing funds in startups and placing them on currency exchange platforms.

B. Fraud on currency exchange platforms. Thus, D. Shabalin D. and M. Orlov, being in a rented apartment in Surgut, Khanty-Mansiysk Autonomous Okrug - Yugra, Tyumen Oblast, connected to the Internet, bought from an unidentified person the vb_user table, containing encrypted access logins and passwords for user accounts and then decrypted them via the Internet in order to steal property of citizens, namely BTC-e codes.

Then, using unidentified means of hiding the IP address, they illegally accessed the user accounts of wmalliance, Djin37 and other unidentified user accounts of a website, after which, using the decrypted login and password, changed information about the user wmalliance and created the topic "BTS-e / Bitcoins withdrawal. + 7% " and positive comments to it on his behalf. D. Shabalin and M. Orlov did the same on behalf Djin37 and other unidentified users of a website.

Further, with the aim of obtaining illegal profit, intending to steal BTC-e codes from an unknown user of a website with an account serl98, they misled the latter, promising him to exchange the BTC-e code for Russian rubles, which they obviously did not intend to do. As a result, serl98, being misled about the criminal intentions of D. Shabalin and M. Orlov, using his own account "serl98" on a website for exchanging the BTC-e code for 10,000 US dollars for Russian rubles, in a personal message conveyed to the user wmalliance, to which D. Shabalin . had access. and M. Orlov, BTC-e code for 10,000 US dollars, the market value of which, according to the expert's opinion, was 821,100 rubles 00 kopecks. Then D. Shabalin and M. Orlov credited the BTC-e code for 10,000 US dollars, owned by serl98, to their account, thereby stole the BTC-e code and then used it at their discretion, thereby causing serl98 material damage of 821,100 rubles.

C. Fake websites. For example, when displaying a website, there is no padlock icon in the browser address bar, "https" is not displayed in the site address. In addition, during automatic redirects a user does not check URLs or type them in.
D. Fake mobile cryptocurrency applications hosted on Google Play and Apple App Store. Though such applications are usually quickly recognized and blocked by site developers, they can be already downloaded by users.

E. Scam e-letters for following a link or for posting information about the initial placement of cryptocurrency.
6. The largest category of cybercrimes involving cryptocurrencies is associated with hacker attacks on cryptocurrency exchanges through the creation, use and distribution of malicious computer programs and subsequently further with cryptocurrencies theft, or phishing.

Conclusions

1. The reference to cryptocurrency anonymity is incorrect. Indeed, it is difficult to identify the user by the cryptocurrency address. However, all the address's transactions are easily traceable, including up to the first transaction, so they are all connected and stored forever, which is the peculiarity of the blockchain. Besides, for the first time, the Office of Foreign Assets Control (OFAC) in the United States linked addresses to the individuals' identity, providing standard data on the place of residence and their passport numbers.

Also, the Federal Financial Monitoring Service has tested the "Transparent Blockchain" project to track transactions in the Bitcoin blockchain related to drug trafficking. The prototype was developed jointly with the P. Lebedev Physical Institute of the Russian Academy of Sciences.

2. The effectiveness of criminal prosecution is impossible without the law enforcement agencies' actions aimed at compensating the damage caused by the crime and at the correct classification of crimes, which is significantly influenced by the legal regulation of digital rights and their market.
If speaking about the compensation for damage, it is worth noting the actual success associated with the authorities and officials' carrying out criminal prosecution drive for such actions (Ivanov et al., 2020; Ivanov & Kruglikov, 2020).

The solution to the issue of qualifications may be in the term "*digital rights*" represented in the Resolution of the Plenum of the Supreme Court of the Russian Federation dated 7, July, 2015 No. 32, as a general term that includes less successful and largely contradictory, however, often used terms "virtual money" and "virtual assets", as well as the terms "cryptocurrencies", "tokens", "stablecoins" *which are used or can be used in cyberspace as a means of exchange and has a specific market value at the time of any transaction*.

This definition has several advantages compared to the definition developed by the US FBI for "virtual currencies" (Federal Bureau of Investigations: Bitcoin Virtual Currency). Firstly, the term "digital rights" is more precise and covers a broader category of virtual rights, assets, currency, securities and their derivatives, weapons and armor in computer games, and so on. Thus, the proposed term takes into account all possible variety *of what is or can be used in cyberspace as a means of exchange and has a specific market value at the time of any transaction*, and consequently can be subject to legalization (laundering) of income. Secondly, two forms of action are implied: active and passive. Thirdly, the opportunity of being used in cyberspace, not only on the Internet, is taken into account, while it (this opportunity) is not the main feature, since the exchange can also take place offline, when an external media containing the digital rights, for example, any cryptocurrency, are given to the suspect or the accused. Fourthly, the issue of determining the cost of digital rights is removed from the agenda, which is especially important in the context of then digital rights high volatility. Fifthly, the US FBI made a serious mistake by not predicting the development of the situation with the inclusion of states in the development of the digital economy and the further approval of certain cryptocurrencies, the creation of their own, therefore the sign "but not supported by the government" should be excluded. Although, when constructing the corresponding corpora delicti in criminal codes, this sign can be taken into account as qualifying. Finally, this kind of definition is extremely demanded by the judicial and investigative practice and does not contradict the development and normative consolidation of a civilistic approach to these issues, which can last as long as it is necessary.

3. Attention to changes in the current criminal procedural legislation aimed at digitalizing the criminal proceedings procedures is required, with the goal to harmonize the relations, being developed in this area.

References

Crypto money laundering up threefold in 2018: Report. The American Banker. [Электронный ресурс]. URL://https://www.americanbanker.com/news/crypto-money-laundering-rose-3x-in-first-half-2018-report (дата обращения: 01.01.2020).

Federal Bureau of Investigations: Bitcoin Virtual Currency: Intelligence Unique Features Present Distinct Challenges for Deterring Illicit Activity. – 24 April 2012. - Intelligence Assessment: Unclassified//for official use only/ - P. 20.

Ivanov, D.A., & Kruglikov, M.A. (2020). Mezhdunarodnyye standarty mer presecheniya i ikh implementatsiya v zakonodatel'stvo Rossiyskoy Federatsii. *Vserossiyskiy kriminologicheskiy zhurnal, 14*(4), 623-630.

Ivanov, D.A., Esina, A.S., Fadeev, P.V., Chasovnikova, O.G., Zorina, E.A. (2020). Crime victim compensation. *Revista Gênero e Direito, 9*(4), 753-759.